# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://sacosta.idte.app | Checks | 9 pruebas |
| Dominio | sacosta.idte.app | Hallazgos | 46 totales |
| Fecha | 12 de mayo de 2026 a las 22:40 | Problemas | 14 detectados |

**D**

55/100

puntos de seguridad

## RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web ha arrojado una puntuación de 55/100, lo que corresponde a una calificación de grado D. El análisis se basó en la ejecución de 9 comprobaciones pasivas, resultando en 4 verificaciones superadas, 3 advertencias y 2 fallos críticos de configuración. Se han identificado carencias importantes en la implementación de políticas de seguridad del lado del servidor y en la gestión del tráfico cifrado. Por tanto, se concluye que el sitio es actualmente vulnerable ante diversos vectores de ataque comunes en la web.

## Resumen de Riesgos

| 0 | 5 | 6 | 3 | 32 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 37 dias |
| Cabeceras de Seguridad | 0 | FALLO | Solo 0/6 presentes. Faltan: Content-Security-Pol... |
| Redireccion HTTPS | 0 | FALLO | No hay redireccion HTTP a HTTPS |
| Deteccion CMS | 100 | OK | No se detecto un CMS conocido |
| Version CMS Expuesta | 100 | OK | No se detecto version de CMS expuesta |
| Seguridad de Cookies | 100 | OK | No se encontraron cookies |
| Contenido Mixto | 60 | AVISO | 1 recurso(s) HTTP en pagina HTTPS |
| Robots.txt y Sitemap | 60 | AVISO | Falta sitemap.xml |
| Puertos Abiertos | 60 | AVISO | 1 puerto(s) potencialmente riesgoso(s): 8080 (HT... |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 37 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  37 dias restantes (expira: 2026-06-18T17:09:21.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-20T16:11:35.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.4.19 — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

## Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

## Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  PHP/8.4.19

## Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

## Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

## Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (CSS url())**
  http://fonts.googleapis.com/css?family=Open+Sans:400,700

## Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1738 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

## Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- INFO **Puerto 22 (SSH)**
  Cerrado — Acceso remoto seguro
- INFO **Puerto 23 (Telnet)**
  Cerrado — Acceso remoto sin cifrar
- INFO **Puerto 25 (SMTP)**
  Cerrado — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — Servidor web seguro
- INFO **Puerto 3306 (MySQL)**
  Cerrado — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- INFO **Puerto 6379 (Redis)**
  Cerrado — Cache Redis sin autenticacion por defecto
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

## Analisis de Seguridad

## VULNERABILIDADES DETECTADAS

[HIGH] Ausencia de Content-Security-Policy: La falta de esta cabecera facilita ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] Falta de X-Frame-Options: Permite que el sitio sea cargado en iframes ajenos, exponiendo a los usuarios a ataques de clickjacking.
[HIGH] Strict-Transport-Security no configurado: El servidor no obliga al navegador a usar conexiones seguras, permitiendo ataques de interceptación.
[HIGH] Fallo en redirección HTTP a HTTPS: El sitio permite el acceso mediante el protocolo HTTP no cifrado sin redirigir automáticamente a la versión segura.
[MEDIUM] Contenido mixto detectado: Se carga un recurso de Google Fonts a través de una conexión HTTP insegura dentro de la página HTTPS.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto alternativo aumenta la superficie de ataque y puede revelar servicios internos.
[MEDIUM] Falta de X-Content-Type-Options: El navegador podría intentar interpretar archivos como un tipo MIME distinto al declarado, facilitando la ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy no establecido: No existe control sobre la información de navegación que se envía a otros sitios web mediante los enlaces.
[MEDIUM] Permissions-Policy ausente: No se restringe el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[MEDIUM] Configuración de robots.txt restrictiva: El archivo bloquea el acceso a todo el sitio, lo cual suele ser una configuración errónea para sitios públicos.
[LOW] Exposición de cabecera Server: Se revela que el sitio utiliza la tecnología Cloudflare, ayudando a un atacante a identificar la infraestructura.
[LOW] Exposición de cabecera X-Powered-By: Se muestra explícitamente el uso de PHP/8.4.19, permitiendo la búsqueda de vulnerabilidades específicas para esta versión.
[LOW] Sitemap.xml no encontrado: La ausencia de este archivo dificulta la auditoría de rutas y la indexación correcta de los contenidos del sitio.